1   41. A method for use by a device operating on a network over which

2 multiple devices belonging to a defined set communicate with each other by

3 transmitting and receiving messages, the method comprising:

4   transmitting the messages at a frequency that hops from one frequency to

5 another over time in accordance with a predictable hopping sequence that

6 determines each frequency in the hopping sequence from a particular identifier

7 associated with one of the devices and a universal time parameter;

8   characterized in that:

9   each frequency in the hopping sequence is determined from a known

10 function of the particular identifier, the universal time parameter, and a seed that

11 changes the hopping sequence from that which would otherwise be determined

12 from the particular identifier and the universal time parameter alone, whereby a

13 pattern of changing transmit frequencies that is detected in messages received

14 by a device outside the defined set is impeded from being associated with the

15 particular identifier associated with one of the devices within the set.

[New Claim 42:]

1   42. The method of claim 41 wherein the seed is changed over time.

[New Claim 43:]

1   43. The method of claim 42 wherein the seed is changed periodically.

[New Claim 44:]

1   44. The method of claim 42 wherein the seed is changed aperiodically.

[New Claim 45:]

1   45. The method of claim 42 wherein the seed is changed when a new

2 session begins on one of the devices in the set.

[New Claim 46:]

1   46. The method of claim 41 wherein the known function is a one-way

2 function.

[New Claim 47:]

1   47. The method of claim 41 wherein the seed is at least a first random or

2   pseudo-random number.

[New Claim 48:]

1   48. The method of claim 45 wherein the seed is at least a first random or

2   pseudo-random number that determines in part the sequence of frequencies in

3   the hopping sequence used for transmitting messages within a current session.

[New Claim 49:]

1   49. The method of claim 47 wherein the seed is a combination of the first

2   random or pseudo-random number and at least a second random or pseudo-

3   random number that determined in part the sequence of frequencies in the

4   hopping sequence used for transmitting messages within at least one previous

5   session.

[New Claim 50:]

1   50. The method of claim 47 wherein the random or pseudo-random

2   number is received in an encrypted form by the device from one of the other

3   devices in the set, and the encrypted random or pseudo-random number is

4   decrypted before being used as the seed.

[New Claim 51:]

1   51. A method for use in a Bluetooth-enabled device operating on a

2   wireless network over which multiple Bluetooth-enabled devices within a defined

3   set communicate with each other by transmitting and receiving messages to and

4   from a master device within the set, the method comprising:

5   transmitting the messages at a frequency that hops from one frequency to

6   another over time in accordance with a predictable hopping sequence that

7   determines each frequency within the hopping sequence from a Bluetooth

8   address (BD_ADDR) associated with the master device and a universal time

9   parameter;

10   characterized in that:

11   each frequency in the hopping sequence is determined from a known

12   function of the master device's BD_ADDR, the universal time parameter, and a

13   seed that changes the hopping sequence from that which would otherwise be

14   determined from the master device's BD_ADDR and the universal time

15   parameter alone, whereby a pattern of changing transmit frequencies that is

16   detected in messages received by a device outside the defined set is impeded

17   from being associated with the master device's BD_ADDR.

[New Claim 52:]

1   52. The method of claim 51 wherein the seed is changed over time.

[New Claim 53:]

1   53. The method of claim 52 wherein the seed is changed periodically.

[New Claim 54:]

1   54. The method of claim 52 wherein the seed is changed aperiodically.

[New Claim 55:]

1   55. The method of claim 52 wherein the seed is changed when a new

2   session begins on one of the devices in the set.

[New Claim 56:]

1   56. The method of claim 51 wherein the known function is a one-way

2   function.

[New Claim 57:]

1   57. The method of claim 51 wherein the seed is at least a first random or

2   pseudo-random number.

[New Claim 58:]

1   58. The method of claim 55 wherein the seed is at least a first random or

2   pseudo-random number that determines in part the sequence of frequencies in

3   the hopping sequence used for transmitting messages within a current session.

[New Claim 59:]

1   59. The method of claim 57 wherein the seed is a combination of the first

2   random or pseudo-random number and at least a second random or pseudo-

3   random number that determined in part the sequence of frequencies in the

4   hopping sequence used for transmitting messages within at least one previous

5   session.

[New Claim 60:]

1   60. The method of claim 57 wherein the random or pseudo-random

2   number is received in an encrypted form by the device from one of the other

3   devices in the set, and the encrypted random or pseudo-random number is

4   decrypted before being used as the seed.

[New Claim 61:]

1   61. Apparatus for use in a device operating on a network over which

2   multiple devices belonging to a defined set communicate with each other by

3   transmitting and receiving messages, the apparatus comprising:

4   means for transmitting the messages at a frequency that hops from one

5   frequency to another over time in accordance with a predictable hopping

6   sequence; and

7   means for determining each frequency in the hopping sequence from a

8   known function of a particular identifier associated with one of the devices in the

9   set, a universal time parameter, and a seed, whereby a pattern of changing

10   transmit frequencies that is detected in messages received by a device outside

11   the defined set is impeded from being associated with the particular identifier

12   associated with one of the devices within the set.

[New Claim 62:]

1   62. The apparatus of claim 61 wherein the seed is changed over time.

[New Claim 63:]

1   63. The apparatus of claim 62 wherein the seed is changed periodically.

[New Claim 64:]

1   64. The apparatus of claim 62 wherein the seed is changed aperiodically.

[New Claim 65:]

1   65. The apparatus of claim 62 wherein the seed is changed when a new

2   session begins on one of the devices in the set.

[New Claim 66:]

1   66. The apparatus of claim of claim 61 wherein the known function is a

2   one-way function.

[New Claim 67:]

1   67. The apparatus of claim 61 wherein the seed is at least a first random

2   or pseudo-random number.

[New Claim 68:]

1   68. The apparatus of claim 65 wherein the seed is at least a first random

2   or pseudo-random number that determines in part the sequence of frequencies in

3   the hopping sequence used for transmitting messages within a current session.

1   **[New Claim 69:]**

2   69. The apparatus of claim 67 wherein the seed is a combination of the

3   first random or pseudo-random number and at least a second random or pseudo-

4   random number that determined in part the sequence of frequencies in the

5   hopping sequence used for transmitting messages within at least one previous

6   session.

[New Claim 70:]

1   70. The apparatus of claim 67 wherein the random or pseudo-random

2   number is received in an encrypted form by the device from one of the other

3   devices in the set, and the processor decrypts the encrypted random or pseudo-

4   random number.

[New Claim 71:]

1   71. Apparatus for use in a Bluetooth-enabled device operating on a

2   wireless network over which multiple Bluetooth-enabled devices within a defined

3   set communicate with each other by transmitting and receiving messages to and

4   from a master device within the set, the apparatus comprising:

5   means for transmitting the messages at a frequency that is hops from one

6   frequency to another over time in accordance with a predicable hopping

7   sequence; and

8   means for determining each frequency in the hopping sequence from a

9   known function of a Bluetooth address (BD_ADDR) associated with the master

10   device, a universal time parameter, and a seed, whereby a pattern of changing

11   transmit frequencies that is detected in messages received by device outside the

12   defined set is impeded from being associated with the master device's

13   BD_ADDR.

[New Claim 72:]

1   72. The apparatus of claim 71 wherein the seed is changed over time.

[New Claim 73:]

1   73. The apparatus of claim 72 wherein the seed is changed periodically.

[New Claim 74:]

1   74. The apparatus of claim 72 wherein the seed is changed aperiodically.

[New Claim 75:]

1   75. The apparatus of claim 72 wherein the seed is changed when a new

2   session begins on one of the devices in the set.

[New Claim 76:]

1   76. The apparatus of claim 71 wherein the known function is a one-way

2   function.

[New Claim 77:]

1   77. The apparatus of claim 71 wherein the seed is at least a first random

2   or pseudo-random number.

[New Claim 78:]

1   78. The apparatus of claim 75 wherein the seed is at least a first random

2   or pseudo-random number that determines in part the sequence of frequencies in

3   the hopping sequence used for transmitting messages within in a current

4   session.

[New Claim 79:]

1   79. The apparatus of claim 77 wherein the seed is a combination of the

2   first random or pseudo-random number and at least a second random or pseudo-

3   random number that determined in part the sequence of frequencies in the

4   hopping sequence used for transmitting messages within at least one previous

5   session.

[New Claim 80:]

1   80. The apparatus of claim 77 wherein the random or pseudo-random

2   number is received in an encrypted from by the device from one of the other

3   devices in the set, and the processor decrypts the encrypted random or pseudo-

4   random number.